Attorney Docket No. 1046.1309

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:

Hiroyuki KOMAI

Application No.: To be Assigned | Group Art Unit: To be Assigned

Filed: February 9, 2004 | Examiner: To be Assigned

For: AUTHENTICATION INFORMATION PROCESSING METHOD

SUBMISSION OF CERTIFIED COPY OF PRIOR FOREIGN APPLICATION IN ACCORDANCE WITH THE REQUIREMENTS OF 37 C.F.R. § 1.55

Commissioner for Patents
PO Box 1450
Alexandria, VA 22313-1450

Sir:

In accordance with the provisions of 37 C.F.R. § 1.55, the applicant(s) submit(s) herewith a certified copy of the following foreign application:

Japanese Patent Application No(s). 2003-37150

Filed: February 14, 2003

It is respectfully requested that the applicant(s) be given the benefit of the foreign filing date(s) as evidenced by the certified papers attached hereto, in accordance with the requirements of 35 U.S.C. § 119.

Respectfully submitted,

STAAS & HALSEY LLP

Date: Feb 9, 2004 By: _____

Gene M. Garner II
Registration No. 34,172

1201 New York Ave, N.W., Suite 700
Washington, D.C. 20005
Telephone: (202) 434-1500
Facsimile: (202) 434-1501

opinia

日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２００３年　２月１４日

出願番号
Application Number: 特願２００３－０３７１５０

[ST. 10/C]: [ＪＰ２００３－０３７１５０]

出願人
Applicant(s): 富士通株式会社

２００３年１０月２７日

特許庁長官
Commissioner,
Japan Patent Office 今井康夫

出証番号　出証特２００３－３０８８６４８

【書類名】　特許願
【整理番号】　0253366
【提出日】　平成15年 2月14日
【あて先】　特許庁長官殿
【国際特許分類】　G06F 17/60
【発明の名称】　認証情報処理方法
【請求項の数】　5
【発明者】
　【住所又は居所】　東京都稲城市大字大丸１４０５番地　株式会社富士通パソコンシステムズ内
　【氏名】　駒井　広行
【特許出願人】
　【識別番号】　000005223
　【氏名又は名称】　富士通株式会社
【代理人】
　【識別番号】　100089244
　【弁理士】
　【氏名又は名称】　遠山　勉
【選任した代理人】
　【識別番号】　100090516
　【弁理士】
　【氏名又は名称】　松倉　秀実
　【連絡先】　０３－３６６９－６５７１
【手数料の表示】
　【予納台帳番号】　012092
　【納付金額】　21,000円
【提出物件の目録】
　【物件名】　明細書　1
　【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9705606

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　認証情報処理方法

【特許請求の範囲】

【請求項１】

ログインを要求するユーザ端末の端末情報を取得するステップと、

前記端末情報に基づき、当該ユーザ端末からのログイン手順を決定するステップと、

前記ユーザ端末からのログイン操作を受け付けるステップと、

前記決定したログイン手順と前記受け付けたログイン操作に基づき前記ユーザ端末からのログインの可否を判定するステップとを備える、認証情報処理方法。

【請求項２】

前記ユーザ端末からの累積ログイン回数を前記端末情報に関連付けて記憶するステップをさらに備え、

前記ログイン手順を決定するステップでは、

前記累積ログイン回数に応じて、前記ログイン手順を決定する、請求項１に記載の認証情報処理方法。

【請求項３】

前記ユーザ端末からの最終ログイン時点を前記端末情報に関連付けて記憶するステップをさらに備え、

前記ログイン手順を決定するステップでは、

前記最終ログイン時点からの経過期間に応じて、前記ログイン手順を決定する、請求項１または２に記載の認証情報処理方法。

【請求項４】

コンピュータに認証情報を処理させる認証情報処理プログラムであり、

ログインを要求するユーザ端末の端末情報を取得するステップと、

前記端末情報に基づき、当該ユーザ端末からのログイン手順を決定するステップと、

前記ユーザ端末からのログイン操作を受け付けるステップと、

前記前記決定したログイン手順と前記受け付けたログイン操作に基づき前記ユ

ーザ端末からのログインの可否を判定するステップとを備える、認証情報処理プログラム。

【請求項５】

ログインを要求するユーザ端末の端末情報を取得する端末情報取得手段と、

前記端末情報に基づき、当該ユーザ端末からのログイン手順を決定するログイン手順決定手段と、

前記ユーザ端末からのログイン操作を受け付けるログイン受付手段と、

前記決定したログイン手順と前記受け付けたログイン操作に基づき前記ユーザ端末からのログインの可否を判定するログイン判定手段と、を有する認証情報処理装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は認証情報処理技術に関する。

【０００２】

【従来の技術】

一般に、コンピュータ等の各種情報処理装置（以下ユーザ端末とする）からネットワークを介してサーバに接続して運用される各種システム(Webページの利用、各種アプリケーションの利用等を含む)がある。通常、このようなシステムでは、他人による不正利用を防止するために、パスワードやＩＤ番号等の認証情報の入力を必要とする。

【０００３】

上記システムでは、ユーザ名やパスワード等の個人情報は、サーバ側で一括管理する。そして、ユーザ側は、必要に応じてサーバにログイン（接続）操作をする。ログイン操作を受け付けたサーバは、当該ユーザからのログイン操作の認証処理をする。上記サーバによって、当該ユーザからのログイン操作が認証されると、ユーザは上記システムを利用可能となる。

【０００４】

通常、上記認証処理は、ユーザ名或いはパスワード等の認証情報を入力するだ

けで、サーバに接続可能な全ての端末からログインできた。そのため、上記システムでは、サーバへの不正侵入の防止等、セキュリティの確保が十分でなかった。従って、従来のシステムでは、ユーザ情報等の、各種情報漏洩の可能性があった。

【０００５】

このような多数のユーザ端末からのログインを受け付けるシステムのセキュリティの維持方法として、例えば以下の方法が挙げられる。

【０００６】

まず、ユーザ名或いはパスワード以外の、他の認証情報を入力させるログイン手順も鑑みられている。

【０００７】

例えば、上記ログイン手順として、パスワードを入力するものがある。また、他のログイン手順として、キーワード（例：ユーザの個人情報をキーワードとして予め設定しておき、このキーワードを尋ねる）をランダムに表示して、毎回入力する文字を変更するものがある。この他の手順には、指紋認証や個人を特定できるIDカード（スマートカード等）を使用するものがある。さらに、ログイン手順には、ログイン操作のタイミングによってログインを許可するといったものがある。

【０００８】

上記のような、ログイン手順の追加によるセキュリティレベルの維持技術以外には、例えば以下の技術が鑑みられている。

【０００９】

まず、上記技術として、ログイン時のパスワードを、適時自動的に変更する技術が開示されている（例えば、特許文献１及び特許文献５参照）。

【００１０】

また、上記技術として、認証済みのユーザからのログイン操作に対して、次回からの認証を簡易認証で行う、簡易認証に係る技術も開示されている（例えば、特許文献２参照）。

【００１１】

さらに、上記技術として、同一のユーザIDを利用する複数の利用者のうち、セキュリティレベルで決まる特定の利用者だけがログインできる、ログイン制御に係る技術も開示されている（例えば、特許文献３参照）。

【００１２】

また、上記技術として、ログイン時の通信路のセキュリティレベルを判定して、コマンド実行の可否を判定するログイン方式に係る技術も開示されている（例えば、特許文献４参照）。

【００１３】

また、上記技術として、ユーザにより指定されるユーザID及びパスワードと、認証システムにより予め設定されるキー文字列とによる、ユーザ認証に係る技術も開示されている（例えば、特許文献６参照）。

【００１４】

【特許文献１】

特開平７－１６０６３８号公報

【特許文献２】

特開２０００－３６８０９号公報

【特許文献３】

特開平４－２７７８５５号公報

【特許文献４】

特開平６－３３７８４４号公報

【特許文献５】

特開平７－１８２０６４号公報

【特許文献６】

特開２００１－２７３２５９号公報

【発明が解決しようとする課題】

しかしながら、上記した各種ログイン手順では、不特定の端末から、決められたログイン手順を実行することで、ログインすることができた。従って、上記ログイン手順を解読された場合には、何者かにシステムを不正利用されるおそれがあった。

【００１５】

また、自動的にパスワードないしキー文字列を変化させたとしても、正規のユーザを特定する情報はユーザID等であるため、ユーザIDを取得した何者かによって、不正利用されるおそれがあった。

【００１６】

さらに、セキュリティを維持するために多数のログイン手順を設けることは、継続的にシステムを利用するにあたり、正規のユーザの利便性を低下させるおそれがあった。

【００１７】

本発明は、前記した事項に鑑みて為されたものであり、ログイン等のユーザ認証のセキュリティと、正規のユーザに対する利便性とを維持することができる、認証情報処理技術を提供することを課題とする。

【００１８】

【課題を解決するための手段】

前記した課題を解決するために、本発明は以下の手段とした。

【００１９】

即ち、本発明では、ログインを要求するユーザ端末の端末情報を取得する。そして、本発明は、前記端末情報に基づき、当該ユーザ端末からのログイン手順を決定する。また、本発明は、前記ユーザ端末からのログイン操作を受け付ける。そして、本発明では、前記決定したログイン手順と前記受け付けたログイン操作に基づき、前記ユーザ端末からのログインの可否を判定する。

【００２０】

本発明では、ログインを要求するユーザ端末を特定して、当該ユーザ端末に対応したログイン手順を決定する。

【００２１】

従って、本発明によれば、不特定の端末からのログイン要求を防止するため、不正侵入等に対するシステムの安全性を維持することができる。

【００２２】

また、本発明は、前記ユーザ端末からの累積ログイン回数を前記端末情報に関

連付けて記憶してもよい。このとき、本発明では、前記累積ログイン回数に応じて、前記ログイン手順を決定する。

【００２３】

従って、本発明によれば、特定のユーザ端末からの正当なログイン回数に応じて、当該ユーザ端末に対するログイン手順を決定するため、正当なログイン操作を継続するユーザのログイン操作を軽減させることができる。

【００２４】

また、本発明は、前記ユーザ端末からの最終ログイン時点を前記端末情報に関連付けて記憶してもよい。このとき、本発明では、前記最終ログイン時点からの経過期間に応じて、前記ログイン手順を決定する。

【００２５】

従って、本発明によれば、最終ログイン時点からの経過期間に応じて、前記ユーザ端末のログイン手順を変化させるため、システムの安全性を維持することができる。

【００２６】

また、本発明は、以上の何れかの機能を実現させるプログラムであってもよい。また、本発明は、そのようなプログラムをコンピュータが読み取り可能な記憶媒体に記録してもよい。

【００２７】

さらに、本発明は、以上の何れかの機能を実現する装置であってもよい。

【発明の実施の形態】

以下、本発明である、認証情報処理方法の一実施の形態について図面を参照して説明する。本実施の形態では、本発明の認証情報処理方法を、実現するために、認証情報処理プログラムを用いる。そして、本実施の形態では、システムを管理するサーバ等の情報処理装置に、この認証情報処理プログラムを導入（インストール）して認証情報処理装置とする。本システムを利用するユーザ側のユーザ端末は、上記認証情報処理装置にログイン（接続）する。認証情報処理装置は、正規のログイン手順を行ったときに、当該ユーザが本システムを利用可能であると判定する。

【００２８】

なお、ユーザ端末が認証情報処理装置の本システムにアクセス可能に接続することは、ログオンとも呼ばれ、本発明においてこれらは同等である。

【００２９】

〈システム構成〉

図１は、本発明の認証情報処理方法を実施するシステムの概略構成図である。本システムは、システムを管理する側の認証情報処理装置１００と、インターネット或いはLAN（Local Area Network）等の各種コンピュータネットワークを介して認証情報処理装置１００に接続する、正規のユーザ端末２００とからなる。また、本システムには、本システムの不正利用を試みる、不正利用者端末３００が、上記各種コンピュータネットワークを介して接続している。

【００３０】

認証情報処理装置１００は、本システムにログインする個々のユーザ端末毎の情報を保持する、管理ファイル１０１を有する。また、認証情報処理装置１００は、ログイン手順及びシステムのセキュリティレベル（不正利用に対する安全性）の情報を関連付けて保持する、セキュリティ定義ファイル１０２を有する。

【００３１】

本実施の形態において、認証情報処理装置１００は、ユーザ端末２００の端末情報を取得する。認証情報処理装置１００は、その端末情報に基づいて、ユーザ端末２００のログイン手順を決定する。そして、認証情報処理装置１００は、決定したログイン手順によるログイン操作を受け付ける。受け付けたログイン操作が正当なものである場合には、認証情報処理装置１００は、このユーザ端末２００のログインを許可する。

【００３２】

〈ファイル構成〉

次に、本装置１００で認証情報処理を実行する際に参照するファイルの構成について説明する。上記ファイルには、ユーザ毎の情報を保持する、管理ファイル１０１と、ログイン手順及びセキュリティレベルを関連付けた、セキュリティ定義ファイル１０２が存在する。

【００３３】

〈管理ファイル〉

図２は、本装置１００が保持する管理ファイル１０１のファイル構成の一例である。管理ファイル１０１は、ユーザ端末２００からのログイン要求とともに端末情報を取得し照合を行うときに、本装置１００が参照するファイルである。本装置１００には、本システムにログインする個々のユーザ端末２００に対応する数のファイルが存在する。

【００３４】

図２に示すように、管理ファイル１０１には、ＭＡＣ（Media Access Control）アドレス１０１ａ、ＣＰＵ（central processing unit）の型番情報１０１ｂ、メモリの型番情報１０１ｃ、最終ログイン日時（本発明の最終ログイン時点の情報）１０１ｄ、システムへの累積ログイン回数１０１ｅ、本システムへのログイン失敗回数１０１ｆ等の、個々のユーザ端末２００毎の端末情報が保持されている。

【００３５】

ユーザ端末２００のMACアドレス１０１ａは、本装置１００がユーザ端末２００を特定するために用いられる。このＭＡＣアドレス１０１ａは、ネットワークに接続する機器にそれぞれ組み込まれて、ネットワークカードに割り当てられている、固有の識別情報である。

【００３６】

また、ユーザ端末２００に搭載されるＣＰＵの情報１０１ｂは、本装置１００がユーザ端末２００を特定するために用いられる。このＣＰＵの情報１０１ｂとしては、例えば、ＣＰＵの型番、或いはＣＰＵのクロック周波数等が挙げられる。

【００３７】

ユーザ端末２００に搭載されるメモリ１０１ｃの情報としては、例えば、メモリの型番、或いはメモリの全容量の数値等が挙げられる。

【００３８】

また、当該ユーザ端末２００からの最終ログイン日時（本発明の最終ログイン

時点の情報）１０１ｄが保持されている。この最終ログイン日時１０１ｄに基づいて、本装置１００がユーザ端末２００のログイン手順を決定する。

【００３９】

そして、当該ユーザ端末２００のシステムへの累積ログイン回数１０１ｅの情報が保持されている。この累積ログイン回数１０１ｅに基づいて、本装置１００がユーザ端末２００のログイン手順を決定する。

【００４０】

さらに、管理ファイル１０１には、本システムへのログイン失敗回数１０１ｆの情報が保持されている。このログイン失敗回数１０１ｆに基づいて、本装置１００がユーザ端末２００のログイン手順のレベルを引き上げるか否かを決定する。

【００４１】

本装置１００は、ユーザ端末２００からのログイン要求を受け付けた場合には、当該ユーザ端末２００の端末情報を取得する。本装置１００は、当該端末情報と、管理ファイル１０１内のMACアドレス１０１ａ、ＣＰＵ１０１ｂ、及びメモリ１０１ｃの情報とを参照し、このマシンがログイン可能なユーザ端末２００であるか否かを判定する。

【００４２】

当該ユーザ端末２００がログイン可能な端末である場合に、本装置１００は、以下の処理を行う。

【００４３】

本装置１００は、当該ユーザ端末２００のログイン手順を、最終ログイン日時１０１ｄまたは累積ログイン回数１０１ｅの情報を参照して、セキュリティ定義ファイル１０２から索出し決定する。なお、セキュリティ定義ファイル１０２の詳細な説明については後述する。

【００４４】

また、本装置１００は、当該ユーザ端末２００がログインを失敗する度にログイン失敗回数１０１ｆを加算する。本装置１００は、このログイン失敗回数１０１ｆが一定回数に到達したときに、当該ユーザ端末２００からのログイン手順を

変更してセキュリティレベルを強化する。

【００４５】

〈セキュリティ定義ファイル〉

図３、図４及び図５は、本装置１００が保持するセキュリティ定義ファイル１０２のファイル構成の一例である。また、図６は、セキュリティレベルをログイン手順と関連付けて保持する、ログイン手順データテーブル１０２ｃの一例である。

【００４６】

セキュリティ定義ファイル１０２は、本装置１００が累積ログイン回数ないし最終ログイン時点から、ユーザ端末２００のログイン手順を決定するためのセキュリティレベルを定義したファイルである。本セキュリティレベルは、その値が大きいほどセキュリティが高いことを示す。

【００４７】

図３に示すセキュリティ定義ファイル１０２ａでは、累積ログイン回数とセキュリティレベルとが関連付けて保持される。セキュリティ定義ファイル１０２ａにおいて、例えば、累積ログイン回数が３から５回までであれば、セキュリティレベル４と定義し、累積ログイン回数が１１から２０回までであれば、セキュリティレベル２と定義する。即ち、本装置１００は、当初累積ログイン回数が少ないときには、当該ユーザ端末２００のセキュリティレベルを高く設定する。その後、本装置１００は、当該ユーザ端末２００からの累積ログイン回数が多くなると、対応するセキュリティレベルを引き下げる。なお、本発明において、この累積ログイン回数とセキュリティレベルとの対応関係は、本実施の形態に限定されることなく、適宜設定することができる。

【００４８】

また、図４に示すセキュリティ定義ファイル１０２ｂでは、最終ログイン時点とセキュリティレベルとが関連付けられて保持される。セキュリティ定義ファイル１０２ｂにおいて、例えば、最終ログイン時点からの経過日数が６から１０日であれば、セキュリティレベル３と定義し、最終ログイン時点からの経過日数が２１日以上であれば、セキュリティレベル５と定義する。即ち、本装置１００は

、当該ユーザ端末２００からの最終ログイン時点からの経過日数が長いときには、対応するセキュリティレベルを引き上げる。また、本装置１００は、当該ユーザ端末２００からの最終ログイン時点からの経過日数が短いときには、対応するセキュリティレベルを引き下げる。なお、本発明において、この最終ログイン時点とセキュリティレベルとの対応関係は、本実施の形態に限定されることなく、適宜設定することができる。

【００４９】

本実施の形態では、本装置１００はユーザ端末２００の累積ログイン回数に該当するセキュリティレベルをセキュリティ定義ファイル１０２ａから決定する。また、本装置１００は、最終ログイン時点からの経過日数を、セキュリティ定義ファイル１０２ｂから決定する。そして、本装置１００は、累積ログイン回数に基づくセキュリティレベルと、最終ログイン時点からの経過日数に基づくセキュリティレベルのうち、セキュリティレベルが高い方を選択してログイン手順に用いる。なお、本発明において、ログイン手順の決定方法は、上述の例に限定されることなく、適宜設定することができる。

【００５０】

図５に示すセキュリティ定義ファイル１０２ｃでは、ログイン失敗回数に応じたセキュリティレベルの変化率の情報が保持されている。セキュリティ定義ファイル１０２ｃにおいて、例えば、ログイン失敗回数が３回までであれば、本装置１００は、セキュリティレベルは現状を維持する。また、ログイン失敗回数が５回であれば、本装置１００は、セキュリティレベルを現状より２段階引き上げる。

【００５１】

即ち、セキュリティ定義ファイル１０２ｃでは、一定の失敗回数に応じてセキュリティレベルの引き上げ幅が定義されている。なお、本発明において、このログイン失敗回数とセキュリティレベルとの対応関係は、本実施の形態に限定されることなく、適宜設定することができる。

【００５２】

図６に示すログイン手順データテーブル１０２ｄは、本装置１００がユーザ端

末２００に要求するログイン手順を定義するテーブルである。このログイン手順データテーブル１０２ｄには、セキュリティレベルに応じたログインの具体的な手順の情報が保持されている。

【００５３】

本実施の形態において、例えば、レベル５のログイン手順は、ユーザ名とパスワード入力による認証、キーワードの入力による認証、指紋による認証、スマートカードによる認証、及び所定のボタンを押している時間による認証である。また、レベル３のログイン手順は、ユーザ名とパスワードの入力による認証、キーワードの入力による認証、指紋による認証である。さらに、レベル１のログイン手順では、ユーザ名とパスワードの入力による認証のみである。

【００５４】

即ち、ログイン手順データテーブル１０２ｄでは、セキュリティレベルに応じて、ログイン手順を軽減させるようにしている。

【００５５】

なお、所定のボタンを押している時間による認証は、以下の方法で行う。まず、本装置１００側では、ユーザ端末２００にあるキーボード上の、予め決められたボタン等を押している時間を予め設定する。そして、本装置１００は、ユーザ端末２００から、ログイン操作時にボタンを押している時間を取得して、取得した時間と予め設定した時間とを照合する。本装置１００は、照合の結果、双方が一致すれば、このユーザ端末２００を認証する。

【００５６】

本装置１００は、このログイン手順データテーブル１０２ｄを、セキュリティ定義ファイル１０２ａ，１０２ｂのうちセキュリティレベルが高い方と対応させて、ユーザ端末２００のログイン手順を決定する。

【００５７】

〈ログイン手順による操作例〉

図７から図１１は、ログイン時の画面推移図の一例である。図７から図１１では、本装置１００がセキュリティレベル５のユーザ端末２００からのログイン操作を受け付ける場合の画面遷移を示す。

【００５８】

まず、システムを使用するユーザは、ユーザ端末２００の図示しないディスプレイに表示される図７のログイン手順操作画面１ａに対して、ユーザ名及びパスワードを入力する。

【００５９】

ユーザ名及びパスワードの認証完了後、本装置１００は当該ユーザ端末２００に、図８のログイン手順操作画面１ｂの画面を表示させる。このログイン手順操作画面１ｂでは、本装置１００はユーザのみが知り得る情報を問う。そのため、この情報と、情報を問うための質問とを予め設定する。なお、本実施の形態では、この情報をキーワードと称する。

【００６０】

ログイン手順操作画面１ｂでは、予めサーバ管理者に通知しておいた複数の質問事項のうち、「好きな動物」についての質問が表示される。ユーザは、ユーザ端末２００に当該質問のキーワードを入力する。本装置１００は、ユーザ端末２００から入力されたキーワードを取得する。そして、予め設定したキーワードと、入力されたキーワードとを比較して認証処理を行う。

【００６１】

キーワードの認証完了後、本装置１００は、ユーザ端末２００に図９のログイン手順操作画面１ｃを表示させる。このログイン手順操作画面１ｃでは、ユーザ端末２００に備えられる図示しない指紋認証システムに、ユーザの指を認識させる。そのため、ユーザ端末２００には、不図示の指紋認証装置を備えている。この指紋認証装置として、例えば、スキャナ等の画像読み取り装置が挙げられる。本装置１００は、この指紋の情報をユーザ端末２００から取得して認証処理を行う。

【００６２】

ユーザ端末２００は、指紋認証装置から読みとった指紋データを本装置１００に送信する。

【００６３】

指紋認証の完了後、本装置１００は、ユーザ端末２００に図１０のログイン手

順操作画面１ｄを表示させる。ログイン手順操作画面１ｄでは、ユーザに渡された図示しないスマートカードを、ユーザ端末２００に読み込ませる。スマートカードとユーザ端末２００との間では、ＰＩＮ（Personal Identification Number）の照合が行われる。

【００６４】

なお、スマートカードとは、ＣＰＵやメモリ、或いはセキュリティ回路といったＩＣチップを組み込んだプラスティックカードのことである。なお、スマートカードは、ＩＣカードと称されることもある。このスマートカードの構造、機能は既知のものであるため、詳細な説明を省略する。

【００６５】

本装置１００において、スマートカードの照合処理に用いた場合、ＰＩＮの照合処理はスマートカードで行う。スマートカードには、設定した正しいＰＩＮが記憶されている。ＰＩＮの照合処理時には、ユーザ端末２００からスマートカードに、入力されたＰＩＮが供給される。スマートカードは、入力されたＰＩＮを予め設定されているＰＩＮと照合する。ＰＩＮの照合が完了すると、ユーザ端末２００は、スマートカードから当該ユーザの認証情報を読み出す。そして、ユーザ端末２００は、スマートカードの認証情報を本装置１００に送信する。

【００６６】

スマートカードによる認証処理完了後、本装置１００は、ユーザ端末２００に図１１のログイン手順操作画面１ｅを表示させる。ログイン手順操作画面１ｅでは、ボタンの押し時間による認証が実行される。ユーザは、ユーザ端末２００に備えられた不図示のボタンに対して、予め設定されたボタンの押し時間である、所定時間（例えば３秒間）のボタン押しを実行する。本装置１００は、このボタンの押し時間が、所定の時間であることを確認して、認証処理を行う。

【００６７】

以上の全ての認証処理完了後、ユーザ端末２００は、本システムに接続することができる。

【００６８】

なお、本実施の形態では、このログイン作業を累積ログイン回数として端末情

報に関連付けて記憶する。このユーザ端末２００から正規のログイン手順操作を継続し続けると、本装置１００は、当該ユーザ端末２００のセキュリティレベルを引き下げて、ログイン手順を簡略化する。

【００６９】

例えば、当初セキュリティレベル５であった場合、一定回数正当なログイン操作を継続することで当該ユーザ端末２００のセキュリティレベルがレベル４になる。このとき、ユーザ端末２００のディスプレイには、ログイン手順操作画面１ｅの画面が表示されなくなる。更に使用を続けることで、当該ユーザ端末２００のセキュリティレベルがレベル３になる。するとログイン手順操作画面１ｄが省略されて、さらに認証処理が簡素化される。

【００７０】

よって、本装置１００によれば、セキュリティレベルを維持しつつ、正規のユーザに対する利便性を維持することができる。

【００７１】

〈ログイン処理〉

図１２は、本装置１００によるログイン処理について説明するフローチャートである。本実施の形態における、認証情報処理（ログイン処理）を、図１２に基づいて説明する。

【００７２】

まず、ユーザ端末２００からログイン要求（図１２におけるステップ１０１、以下Ｓ１０１のように省略する）を受け付けた本装置１００は、当該ユーザ端末２００からの端末情報を取得する。このとき、本装置１００は、上記端末情報を基にして、管理ファイル１０１を検索する。そして、本装置１００は、当該ユーザ端末２００の最終ログイン時点と累積ログイン回数とを参照する。このとき、本装置１００は、双方のセキュリティレベルのうち、セキュリティレベルの高い方（ログイン手順が多い方）を参照する。

【００７３】

また、本装置１００は、当該ユーザ端末２００に関するログイン失敗回数の情報を管理ファイル１０１より取得する。以上の本装置１００による端末情報と管

理ファイル１０１との照合処理を、ユーザ照合処理とする（Ｓ１０２）。

【００７４】

本装置１００は、管理ファイル１０１と関連付けられたセキュリティ定義ファイル１０２を参照して、当該ユーザ端末２００に対する現在のセキュリティレベルを決定する。そして、本装置１００は、決定したセキュリティレベルに応じたログイン手順を、セキュリティ定義ファイル１０２に基づいて決定する（Ｓ１０３）。当該ユーザ端末２００に対して決定したログイン手順を通知して、このログイン手順によるログイン操作を、ログイン手順操作画面を介して要求する。

【００７５】

ユーザは、本装置１００が決定したログイン手順の操作をユーザ端末２００に入力する（Ｓ１０４）。本装置１００は、ユーザ端末２００に入力されたログイン操作を、ネットワークを介して受け付ける。

【００７６】

本装置１００は、受け付けたログイン操作が正当なログイン操作であるか否かを、セキュリティ定義ファイル１０２を参照して判定する（Ｓ１０５）。本装置１００は、このステップ１０５の判定の結果、当該ログイン操作が正当なログイン操作である場合には、累積ログイン回数を１回加算する（Ｓ１０６）。そして、本装置１００は、当該ユーザ端末２００のログインを許可して、認証処理を終了する。

【００７７】

上記ステップ１０５にて、受け付けたログイン操作が正当なログイン操作でないと判定した場合、本装置１００は、管理ファイル１０１のログイン失敗回数を１回加算する（Ｓ１０７）。

【００７８】

そして、本装置１００は、当該ユーザ端末２００のログイン失敗回数が予め設定された一定の回数に到達したか否かを判定する（Ｓ１０８）。このとき当該ログイン失敗回数が一定の回数に到達していない場合には、本装置１００は、ユーザ端末２００に再度ログイン操作を要求するため、ステップ１０４の処理に戻る。

【００７９】

上記ステップ１０８の処理において、当該ログイン失敗回数が一定の回数に到達した場合には、本装置１００は、セキュリティ定義ファイル１０２を参照してセキュリティレベルを引き上げる（Ｓ１０９）。そして、本装置１００は、ユーザ端末２００に再度ログイン操作を要求するため、ステップ１０４の処理に戻る。

【００８０】

このようなログイン処理を行うことによって、本装置１００は、セキュリティレベルを維持しつつ、ユーザの利便性を維持することができる。

【００８１】

〈実施の形態の効果〉

本実施の形態では、ログイン時に行う認証方法を、過去の実績から判断し、セキュリティレベルを変動させている。従って、本実施の形態では、従来のユーザ名とパスワードだけのシステムに比べてセキュリティが強固になる。また、本システムは、正当なログイン操作を継続することで当該ユーザ端末２００のログイン手順を簡略化するので、常に面倒な入力を行う必要がなくなる。従って、本装置１００によれば、ユーザの使い勝手を損なうことなく、不正ログインを防止することができる。

【００８２】

〈変形例〉

なお、本発明の認証情報処理方法は、本実施の形態にのみ限定されるものではなく、本発明の要旨を逸脱しない範囲内において種々変更を加え得ることは勿論である。

【００８３】

例えば、一度不正にログインされた場合、いわゆるハッカーは何度でもそのシステムに侵入することができ、長期的にシステム内の情報を監視できてしまう場合がある。この問題を解決するために、本装置１００の処理を簡単なセキュリティレベルから、強固なセキュリティレベルに移行させてもよい。

【００８４】

図１３は、上記の場合における、ログイン回数が増加するのに応じてセキュリティレベルとログイン手順とを引き上げた、ログイン手順データテーブルの一例である。本処理では、接続回数が多くなればなる程セキュリティのレベルを引き上げる。

【００８５】

通常、ハッカー等の不正利用者は、一度ログインに成功すると、同じログイン手順を用いて再度ログイン操作を試みる。本装置１００は、一度ログインされた場合であっても、ログイン回数に応じてログイン手順を追加していく。よってハッカーによって何度もログインされる場合に、セキュリティレベルが自動的にあがるため、再侵入を防止することできる。

【００８６】

また、本実施の形態において、セキュリティレベルの決定は、当該ユーザ端末２００の累積ログイン回数によるセキュリティレベルと、最終ログイン時点からの経過日数によるセキュリティレベルとを参照して、セキュリティレベルが高い方を当該ユーザ端末２００のセキュリティレベルと決定した。しかしながら、本発明ではこれに限定されることはない。

【００８７】

例えば、累積ログイン回数によって索出されるセキュリティレベルと最終ログイン時点からの経過日数によって索出されるセキュリティレベルのうち、セキュリティレベルの低い方を当該ユーザ端末２００のセキュリティレベルと決定してもよい。

【００８８】

また、例えば、累積ログイン回数によって索出されるセキュリティレベルと最終ログイン時点からの経過日数によって索出されるセキュリティレベルとの平均値を、当該ユーザ端末２００のセキュリティレベルとして決定してもよい。

【００８９】

さらに、例えば、累積ログイン回数によって索出されるセキュリティレベルと、最終ログイン時点からの経過日数によって索出されるセキュリティレベルの何れか一方を、当該ユーザ端末２００のセキュリティレベルとしてもよい。

【００９０】

また、セキュリティレベルを変化させることなく、決定したログイン手順によるログイン操作が正当であった場合に、ユーザ端末２００からのログインを許可してもよい。

【００９１】

さらに、本装置１００は、セキュリティレベルに応じて、ユーザ端末２００のアクセス制限を行ってもよい。

【００９２】

また、セキュリティレベルに応じて、ログイン時にアクセスできるファイルの範囲を決定する、或いは、接続するファイルの書込制限を行ってもよい。

【００９３】

また、セキュリティレベルを索出せずに、累積ログイン回数或いは最終ログイン時点からの経過日数によって、ログイン手順を決定してもよい。

【００９４】

また、認証情報は、図２に例示したものに限定されず、端末を識別可能な情報であれば、その種別、或いは利用する個数はいかなるものであってもよい。

【００９５】

〔その他〕

本発明は、以下のように特定することができる。

【００９６】

（付記１）ログインを要求するユーザ端末の端末情報を取得するステップと、前記端末情報に基づき、当該ユーザ端末からのログイン手順を決定するステップと、前記ユーザ端末からのログイン操作を受け付けるステップと、前記決定したログイン手順と前記受け付けたログイン操作に基づき前記ユーザ端末からのログインの可否を判定するステップとを備える、認証情報処理方法。

【００９７】

（付記２）前記ユーザ端末からの累積ログイン回数を前記端末情報に関連付けて記憶するステップをさらに備え、前記ログイン手順を決定するステップでは、前記累積ログイン回数に応じて、前記ログイン手順を決定する、付記１に記載の

認証情報処理方法。

【００９８】

（付記３）前記ユーザ端末からの最終ログイン時点を前記端末情報に関連付けて記憶するステップをさらに備え、前記ログイン手順を決定するステップでは、前記最終ログイン時点からの経過期間に応じて、前記ログイン手順を決定する、付記１または２に記載の認証情報処理方法。

【００９９】

（付記４）前記端末情報、前記累積ログイン回数、及び前記経過期間の何れかを参照して、前記ユーザ端末に対するセキュリティレベルを決定するステップをさらに備え、前記ログイン手順を決定するステップでは、前記セキュリティレベルに応じて前記ログイン手順を決定する、付記３に記載の認証情報処理方法。

【０１００】

（付記５）ログインを要求するユーザ端末の端末情報を取得する端末情報取得手段と、前記端末情報に基づき、当該ユーザ端末からのログイン手順を決定するログイン手順決定手段と、前記ユーザ端末からのログイン操作を受け付けるログイン受付手段と、前記決定したログイン手順と前記受け付けたログイン操作に基づき前記ユーザ端末からのログインの可否を判定するログイン判定手段と、を有する認証情報処理装置。

【０１０１】

（付記６）前記ユーザ端末からの累積ログイン回数を前記端末情報に関連付けて記憶する累積ログイン回数記憶手段をさらに有し、前記累積ログイン回数に応じて、前記ログイン手順を決定する、付記５に記載の認証情報処理装置。

【０１０２】

（付記７）前記ユーザ端末からの最終ログイン時点を前記端末情報に関連付けて記憶する最終ログイン時点記憶手段をさらに有し、前記最終ログイン時点からの経過期間に応じて、前記ログイン手順を決定する、付記５または６に記載の認証情報処理装置。

【０１０３】

（付記８）前記端末情報、前記累積ログイン回数、及び前記経過期間の何れか

を参照して、前記ユーザ端末に対するセキュリティレベルを決定するセキュリティレベル決定手段をさらに有し、

前記ログイン手順決定手段が、

前記セキュリティレベルに応じて、前記ログイン手順を決定する、付記７に記載の認証情報処理装置。

【０１０４】

（付記９）コンピュータに認証情報を処理させる認証情報処理プログラムであり、ログインを要求するユーザ端末の端末情報を取得するステップと、前記端末情報に基づき、当該ユーザ端末からのログイン手順を決定するステップと、前記ユーザ端末からのログイン操作を受け付けるステップと、前記前記決定したログイン手順と前記受け付けたログイン操作に基づき前記ユーザ端末からのログインの可否を判定するステップとを備える、認証情報処理プログラム。

【０１０５】

（付記１０）前記ユーザ端末からの累積ログイン回数を前記端末情報に関連付けて記憶するステップをさらに備え、前記ログイン手順を決定するステップでは、前記累積ログイン回数に応じて、前記ログイン手順を決定する、付記９に記載の認証情報処理プログラム。

【０１０６】

（付記１１）前記ユーザ端末からの最終ログイン時点を前記端末情報に関連付けて記憶するステップをさらに備え、前記ログイン手順を決定するステップでは、前記最終ログイン時点からの経過期間に応じて、前記ログイン手順を決定する、付記９または１１に記載の認証情報処理プログラム。

【０１０７】

（付記１２）前記端末情報、前記累積ログイン回数、及び前記経過期間の何れかを参照して、前記ユーザ端末に対するセキュリティレベルを決定するステップをさらに備え、

前記ログイン手順を決定するステップでは、

前記セキュリティレベルを参照してセキュリティレベルを決定する、付記１１に記載の認証情報処理プログラム。

【０１０８】

【発明の効果】

以上、説明したように本発明の認証情報処理方法によれば、ログインのセキュリティと、正規のユーザに対する利便性とを維持することができるという優れた効果を奏し得る。

【図面の簡単な説明】

【図１】

本発明の一実施の形態に係る、システムの概略構成図。

【図２】

本実施の形態に係る、認証情報処理装置が保持する管理ファイルのファイル構成の一例。

【図３】

本実施の形態に係る、累積ログイン回数とセキュリティレベルとが関連付けて保持されるセキュリティ定義ファイルの一例。

【図４】

本実施の形態に係る、最終ログイン時点とセキュリティレベルとが関連付けられて保持されるセキュリティ定義ファイルの一例。

【図５】

本実施の形態に係る、ログイン失敗回数とセキュリティレベルとが関連付けられて保持されているセキュリティ定義ファイルの一例。

【図６】

本実施の形態に係る、ログイン手順データテーブルの一例。

【図７】

本実施の形態に係る、ログイン時の画面推移図の一例。

【図８】

本実施の形態に係る、ログイン時の画面推移図の一例。

【図９】

本実施の形態に係る、ログイン時の画面推移図の一例。

【図１０】

本実施の形態に係る、ログイン時の画面推移図の一例。

【図１１】

本実施の形態に係る、ログイン時の画面推移図の一例。

【図１２】

本実施の形態に係る、本装置によるログイン処理について説明するフローチャート。

【図１３】

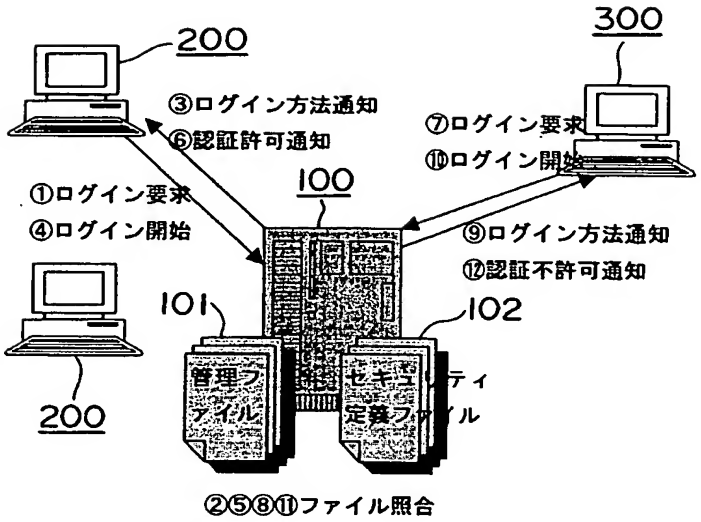
本実施の形態に係る、ログイン回数が増加するのに応じてセキュリティレベルとログイン手順とを増加させたときの、ログイン手順データテーブルの一例。

【符号の説明】

１ａ　ログイン手順操作画面
１ｂ　ログイン手順操作画面
１ｃ　ログイン手順操作画面
１ｄ　ログイン手順操作画面
１ｅ　ログイン手順操作画面
１００　　認証情報処理装置
１０１　　管理ファイル
１０１ａ　ＭＡＣアドレス
１０１ｂ　ＣＰＵ情報
１０１ｃ　メモリ情報
１０１ｄ　最終ログイン日時情報
１０１ｅ　累積ログイン回数情報
１０１ｆ　ログイン失敗回数情報
１０２ａ　セキュリティ定義ファイル
１０２ｂ　セキュリティ定義ファイル
１０２ｃ　セキュリティ定義ファイル
１０２ｄ　ログイン手順データテーブル
２００　　ユーザ端末
３００　　不正利用者端末

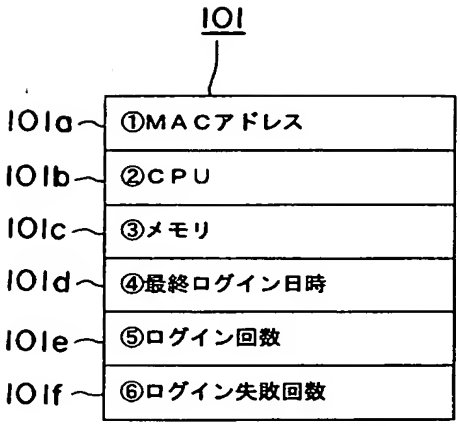
【書類名】　図面

【図１】



本発明の一実施の形態に係る、システムの概略構成図

【図２】



管理ファイルのファイル構成

【図３】

累積ログイン日数	レベル	ログイン手順
1-2	5	レベル５のログイン手順
3-5	4	レベル４のログイン手順
6-10	3	レベル３のログイン手順
11-20	2	レベル２のログイン手順
21	1	レベル１のログイン手順

累積ログイン回数とセキュリティレベルとが
関連付けて保持されるセキュリティ定義ファイル

【図４】

経過日数	ﾚﾍﾞﾙ	ログイン手順
21-	5	レベル５のログイン方法
11-20	4	レベル４のログイン方法
6-10	3	レベル３のログイン方法
3-5	2	レベル２のログイン方法
1-2	1	レベル１のログイン方法

最終ログイン時点とセキュリティレベルとが
関連付けられて保持されるセキュリティ定義ファイル

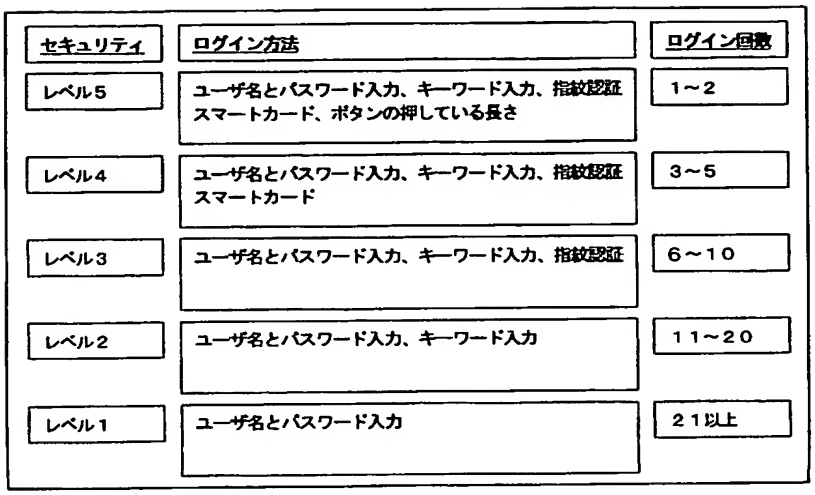
【図５】

102c

失敗回数	セキュリティレベル
0-3	現状維持
4	現状＋１
5	現状＋２
6	現状＋３
7−	現状＋４

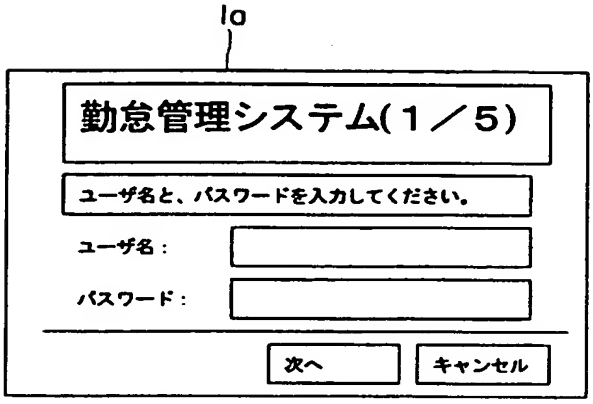
ログイン失敗回数とセキュリティレベルとが
関連付けられて保持されているセキュリティ定義ファイル

【図６】



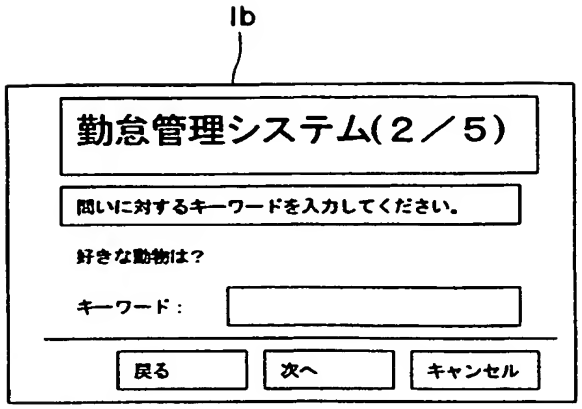
ログイン手順データテーブル

【図７】



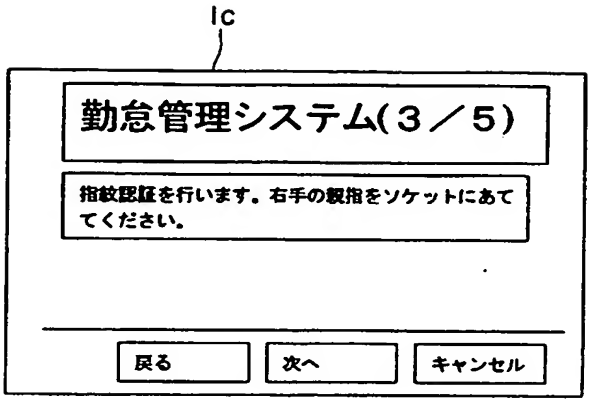
ログイン時の画面推移図

【図８】


Ib
勤怠管理システム(２／５)
問いに対するキーワードを入力してください。
好きな動物は？
キーワード：
戻る
次へ
キャンセル

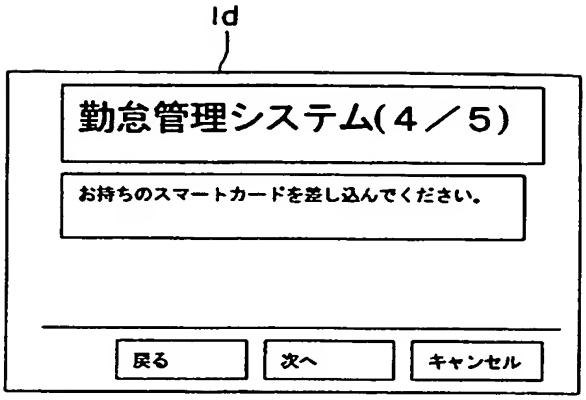
画面推移図

【図９】



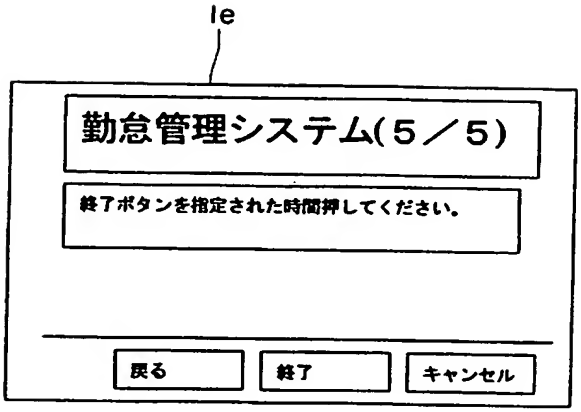
ログイン時の画面推移図

【図１０】



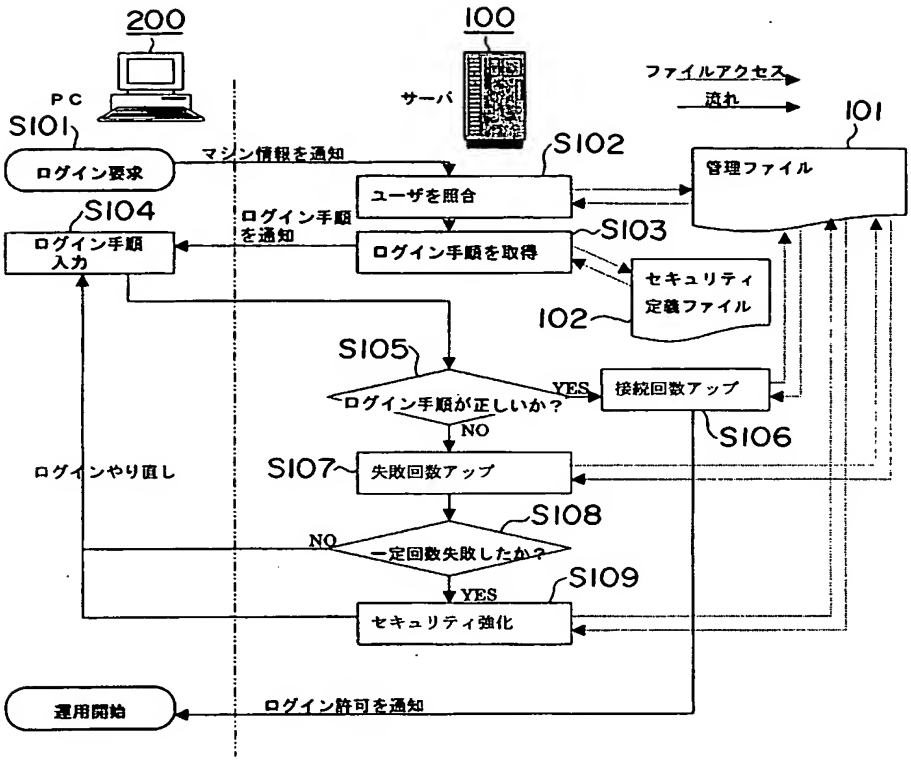
ログイン時の画面推移図

【図１１】



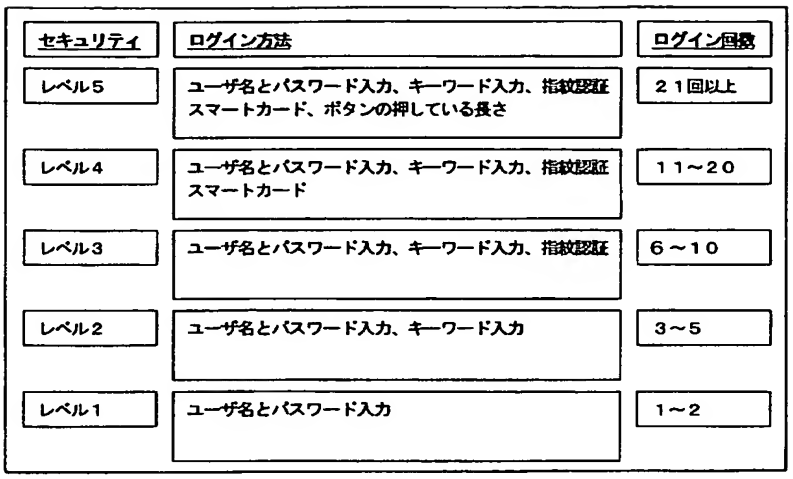
ログイン時の画面推移図

【図１２】



本実施の形態に係る、本装置によるログイン処理のフローチャート

【図１３】



ログイン回数が増加するのに応じて
セキュリティレベルとログイン手順とを増加させたときの、
ログイン手順データテーブル

【書類名】　要約書

【要約】

【課題】　ログインのセキュリティと、正規のユーザに対する利便性とを維持することができる、認証情報処理技術を提供する。

【解決手段】　ログインを要求するユーザ端末の端末情報を取得し、前記端末情報に基づき、当該ユーザ端末からのログイン手順を決定し、前記決定したログイン手順によるログイン操作を受け付け、前記ログイン操作が正当である場合に、前記ユーザ端末からのログインを許可する。

【選択図】　図１

特願２００３－０３７１５０

出　願　人　履　歴　情　報

識別番号　　［０００００５２２３］

１．変更年月日　　１９９６年　３月２６日
［変更理由］　　住所変更
住　所　　神奈川県川崎市中原区上小田中４丁目１番１号
氏　名　　富士通株式会社